Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Tuesday, October 17, 2006

Citron's "data reservoirs": putting liability at the wrong end of the problem

Danielle Citron has written an interesting article on liability for leaks of data like social security numbers (SSNs) that many organizations use as authenticators. Use of such weak authenticators increasingly results in failed (i.e. false) authentication ("identity theft") that harms a victim by imputing to that victims debts or bad credit history. Citron argues that the handling of such "personal data," like the reservoirs in *Rylands v. Fletcher,* should be deemed an "ultrahazardous activity", and thus that those who handle personal data should be held strictly liable for any damages caused in fact by the handling of that data (in particular, by leaks of that data subsequently used by "cyber-criminals" to harm a victim).

There are several things wrong with Citron's analysis:

(1) Strict liability, like other forms of liability, is generally limited by proximate cause. Indeed, I've never heard of strict liability coupled to mere cause-in-fact. If there is a data leak by Trent that enables Mallet to falsely authenicate himself as Bob, which failed authentication is then depended on by Alice resulting in harm to Bob, both Mallet and Alice are intermediate causes of Bob's harm. There is thus cause-in-fact but no proximate cause between Trent's data leak and the harm to Bob. Indeed, the typical identity theft involves a chain of causation quite remote from the data leaker and thus far beyond where courts have ever dared to tread. This is in sharp contrast to the completely unmediated causes in all previous ultrahazardous activity strict liability regimes.

The case Citron cites about the landlord being held liable for the harm of an assault inside his property arose as she states under negligence, not strict liability. Furthermore it was a rare exception, it is not the rule. In most states this would go the other way. The same issue of intermediate cause has rendered futile attempts to hold gun sellers responsible for crimes committed with their guns. The relation between the typical data merchant and the person referred to in the data is far more distant than the landlord/tenant relationship. Even the gun seller is fewer intermediate causes away from the harm of a typical murder than an SSN leaker is to the harm of a typical identity theft victim. Quite often the origin of the identity thief's false authenticator simply cannot be established, whereas the organization that depended on the false authenticator and proximately caused bad credit or false debt is well known.

(2) The article assumes data held by trusted central authorities who have the ability to protect this data at a relatively low cost, and that if they cannot protect it then society could do without the activity. The first assumption is questionable given the existence of tiny data fobs and many other ways to steal or accidentally lose data beyond the control of the organization. Citron debunks the second assumption herself by pointing out how ubiquitous and how important the use of such data is.

Furthermore, just about every organization in our society, and many individuals, handle data which could be used to harm people. It's

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

hard to imagine articulating a rule clear enough (by, say, restricting it to specific kinds of data such as SSNs) to cover most of the risks, yet to put the risks on the major data brokers in particular but not on the rest of us. If strict liability is restricted to certain poor authenticators (e.g. SSNs) but not others (e.g. legal names), data brokers and authenticators will simply switch their activities to use the non-covered authenticators, which are often even weaker, the result being even greater levels of identity theft.

(3) Citron does not provide a clear set of rules, but clear and complely objective rules, and methods for gathering unambiguous evidence of violations, are crucial for a regime of strict liability.

(4) A much better alternative is to let liability lie on organizations that use information known to be widely distributed and often leaked, such as SSNs, as authenticators, and on organizations or individuals who most proximately cause the harm of identity theft -- those who even in good faith falsely report the victim's name to a credit bureau or try to collect a false debt from the victim that was incurred by depending on a false authentication of the victim. These situations are far more analogous to the landlord case -- like the landlord, they have established a relationship with victim; at least they have after falsely reporting the victim's name to a credit bureau or trying to collect a false debt from the victim. Indeed they are more proximate to the victim than even the identity thief: the thief fraudulently used the victim's authenticators, but the thief was not the party that directly harmed the victim by putting the false information on the victim's credit report or by attempting to collect a debt the victim did not in fact incur.

(5) Citron's "data reservoir" metaphor is facially attractive, but as with most physical metaphors applied to information it is highly misleading. The "water" (data) leaking here causes no obvious direct damage like a flood. Rather when data leaks it does not cause any damage until it is used by other parties, like water being used for irrigation. Applying Citron's reasoning to the latest *e. coli* contaminated spinach harm, Citron would make liable not the immediate seller of the spinach, nor the packager, nor even the grower who used the contaminated water. Instead Citron would put the liability on the rancher whose cattle produced the *e. coli* in the first place, even though *e. coli* is inevitable ingredient of manure and thus an inevitable part of ranching activity. Citron's strict liability rule would brinig the entire business of cattle ranching to an end. Just the same, in a world of laptops and fobs and a variety of other conduits, data leaks are an inevitable part of the indispensible business of handling data, and Citron's rue would devastatingly bring this business to an end.

Bottom line: liability should be put on the low-cost avoider. This is not merely a rule of negligence but a guideline for determining where any kind of liability should fall in any new area of commerce. The idea that the data brokers are the low cost avoiders in this system is highly implausible. Rather, here as with most other harms, it is those parties most proximate to the harm who can most easily prevent it. Furthermore, the evidence needed to hold parties liable will be far more reliably available for the proximate harmer than the remote data leaker.

Organizations that use widely distributed and easily leaked data like SSNs as authenticators, and who currently depend on such weak authentications for credit reporting and debt collection, can switch to more secure passwords at lower costs than would be imposed by Citron's regime. Organizations that fail to use secure authenticators, especially organizations that report information to credit bureaus or attempt to collect debts based on insecure authenticators, should bear the liability for identity theft due to the known insecurity of those authenticators, rather than organizations who inevitably leak already widely distributed data.

H/T: Emergent Chaos.

Posted by Nick Szabo at 1:50 AM

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ► November (7)
  - ▼ October (15)
    - Things as authorities
    - Fifty years ago today
    - The pigeonhole principle
    - Three kinds of jurisdiction
    - Citron's "data reservoirs": putting liability at t...
    - How to succeed or fail on a frontier
    - 600,000 excess deaths in Iraq since U.S. invasion
    - Visual mathematics
    - Prosecute U.S. Justice Department lawyers as war c...
    - Hungarian Revolution anniversary
    - Liberty and habeas corpus (II)
    - New fun legal specialty
    - The Lex Gabina: ancient Military Commissions Act?
    - Hello Kitty people
    - Liberty and habeas corpus (I)

Newer Post Home Older Post

- September (15)
- August (20)
- July (5)
- June (10)
- May (4)
- April (3)
- March (11)
- February (10)
- January (26)

- 2005 (44)

Simple theme. Powered by Blogger.